UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,404	11/03/2003	Benjamin Wilken	12221-020001	6346

26161 7590 10/29/2008

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
SQUIRES, BRETT S	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/701,404	WILKEN ET AL.	
	Examiner	Art Unit	
	BRETT SQUIRES	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-17,19-31,33-36* is/are rejected.

7)☒ Claim(s) *5,18,32* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Objections

1. Claims 4, 17, 27, and 31 are objected to as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 4, 17, 27, and 31 recite "more than 'C3' new host pairs," the type of variable "C3" is undefined. The examiner respectfully points to independent claim 1 as an example for defining the type of variables being claimed, independent claim 1 defines variable "C1" as a first threshold number and "C2" as a first factor value. Appropriate correction is required.

2. Claim 5 is objected to because of the following informalities: claim 5 recites "a first threshold number 'C4'," on line 8 and "a first factor value 'C5'," on line 10 it is unclear whether the recited claim limitations are intended to refer to "a first threshold number 'C1'," and "first factor value 'C2'," recited in independent claim 1. Appropriate correction is required.

3. Claim 18 is objected to because of the following informalities: claim 18 recites "a first threshold number 'C4'," on line 19 and "a first factor value 'C5'," on line 20 it is unclear whether the recited claim limitations are intended to refer to "a first threshold number 'C1'," and "first factor value 'C2'," recited in independent claim 14. Appropriate correction is required.

4. Claim 32 is objected to because of the following informalities: claim 32 recites "a first threshold number 'C4'," on line 18 and "a first factor value 'C5'," on line 19 it is unclear whether the recited claim limitations are intended to refer to "a first threshold

number 'C1'," and "first factor value 'C2'," recited in independent claim 28. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4, 6-17, 19-31, and 33-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Pruthi (US 2004/0015581).

Regarding Claims 1, 14, 24, and 28:

Pruthi discloses a method of detecting scanning attacks that adds host-pair connection records to a connection table ("Host-Pairs Table" See fig. 14 ref. no. 1402 and paragraphs 115-116) stored on a computer readable ("Short-term Memory" and "Long-term Memory" See fig. 5 ref. nos. 508 and 510) medium when a host accesses another host, at the end of a first update period accessing the connection table to determine new host pair ("The start field specifies the beginning time from which the traffic is analyzed and its results are displayed on the GUI." and "The stop field specifies the ending time to which the traffic is analyzed and its results are displayed on the GUI." See paragraphs 92-93), determining the number of new host pairs added to the

connection table over the first update period ("The number of IP host pair connections involving a common IP address exceeds x over a time window y." See paragraph 187), and if a host has made more than a first threshold number "C1" host pairs ("Threshold x" See paragraph 187) and an historical number of host pairs is smaller than the threshold number by a first factor value "C2" ("The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, as opposed to alerting the operator that the network is always under scanning attacks when normal operating traffic is on the network." See paragraph 200) then indicating that the new host is a scanner ("Providing a request for action in response to a pattern indicative of an intruder" See paragraphs 172-187).

Regarding Claims 2, 15, 25, and 29:

Pruthi discloses the first threshold number "C1" and the first factor value "C2" are adjustable (See paragraph 200).

Regarding Claims 3, 16, 26, and 30:

Pruthi discloses the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table ("The connection table is continuously updated at the time interval indicated by the operator in the window field when the operator has indicated that the connection table should be continuously updated in the stop field." See fig. 10 ref. nos. 1014-1015 and paragraphs 93-94).

Regarding Claims 4, 13, 17, 27, and 31:

Pruthi discloses aggregating records from the current time-slice table into a second update period table ("The records computed for time interval entered by the operator in the window field, such as 30 seconds, are aggregated over the time interval entered by the operator in the start and stop field, such as 2 hours." See fig. 10 ref. nos. 1013-1015 and paragraphs 92-94), the second update period table having a period that is greater in duration than the first update period (See paragraphs 92-94), checking for ping scans at the end of the second update period ("The method of detecting scanning attacks keeps track of ICMP echo request packets." See paragraph 219) and indicating hosts which produced more than C3 new host pairs over the second update period ("When the number of ping scans detected exceeds the threshold x, the difference between the numbers of ping scans detected and the threshold x corresponds to 'C3'." See paragraph 187).

Regarding Claims 6 and 19:

Pruthi discloses maintaining Address Resolution Protocol packet statistics in the connection table and for sparse subnet tracking the number of generated ARP requests that do not receive response to detect scans on sparse sub-networks ("The examiner respectfully points out that method for detecting scanning attacks can be implement on spare sub-networks." See paragraphs 35, 42, 109, and 202).

Regarding Claim 7:

Pruthi discloses the scanning attack is a ping scanning attack ("The method of detecting scanning attacks keeps track of ICMP echo request packets." See paragraph 219)

Regarding Claims 8, 20, and 33:

Pruthi discloses a method of detecting scanning attacks retrieves from a connection table ("Tables Frame" See fig. 10 ref. no. 1010 and paragraph 90) stored on a computer readable medium ("Short-term Memory" and "Long-term Memory" See fig. 5 ref. nos. 508 and 510) logged values of protocols ("The tables in the table frame are automatically generated based upon protocols found to be active in the specified interval." and "The protocol listed in tables in table frame are selectable by a user to list protocols encapsulated within the selected protocol." See fig. 12 ref. no. 1240, paragraphs 109 and 112) and ports ("The operator can configure the GUI to identify and display connections with an excessive amount of ports being used." and "The operator can configure the GUI to display a specified list of valid ports." See paragraphs 199-206) used in host pair connections records ("Host-Pairs Table" See fig. 14 ref. no. 1402 and paragraphs 115-116) in the connection table, determining if the number of ports used in a historical profile ("The examiner respectfully points out that it is inherent that the operator has access to the historical number of ports scanned during normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, as opposed to alerting the operator that the network is always under scanning attacks when normal operating traffic is on the network." See paragraph 200) is smaller by a factor "C1" than a current number of ports being scanned by a host ("The method of detecting scanning attacks determines in the current number of ports being scanned by a host is smaller than a threshold x number of ports with the difference between the scanned number

and the threshold x number corresponding to a factor 'C1'." See paragraphs 187 and 199-209) and if the current number is greater than a lower-bound "C2" ("Threshold x" See paragraph 187) recording an anomaly and reporting a port scan ("Alert the operator of suspicious activity." See paragraphs 207-209).

Regarding Claims 9, 21, and 34:

Pruthi discloses assigning a severity level to the port scan and reporting the severity level of the port scan ("The port scan has two severity levels; the current number of ports being scanned is smaller than the threshold x number of port and the current number of ports being scanned is larger than the threshold x number. When the number of ports scanned is smaller than x the port scan severity level is low and when the number of ports scanned is larger x the port scan severity level is high." See paragraphs 187 and 199-209)

Regarding Claims 10, 22, and 35:

Pruthi discloses the reported severity varies as a function of the deviation from the historical norm ("The historical norm is selected to be below threshold x, so when the number of ports being scanned is larger the threshold x the number of ports deviates from the historical norm." See paragraphs 187 and 199-209).

Regarding Claims 11, 23, and 36:

Pruthi discloses determining from accessing data in the connection table statistics about TCP reset packets ("Once a packet is identified as TCP the packet is then examined to determine whether it opens or is initiating a TCP connection." See paragraphs 67-68) and ICMP port-unreachable packets ("The network monitor is able to

analyze ICMP traffic and ICMP port unreachable packets are included in ICMP traffic." See paragraph 35), to detect a spike in the number of reset packets and ICMP port-unreachable packets relative to the historical profile to increase the severity of a port scan event (See paragraphs 35, 114, 165, and 219).

Regarding Claim 12:

Pruthi discloses the determining occurs at the end of first duration update periods to detect normal scans ("Time window y" See paragraphs 187-190).

Allowable Subject Matter

7. Claims 5, 18, 32 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

8. Applicant's arguments filed July 17, 2008 have been fully considered but they are not persuasive.

In response to the applicants' argument that Pruthi does not disclose "adding host-pair connection records to a connection table," and therefore Pruthi does not "determine the number of new host pairs added to the table over the first update period." The examiner respectfully points the applicants to Host-Pairs Table shown in figure 14 ref. no. 1402 and paragraphs 115-116. The examiner further points the

applicants to the updating to the Host-Pairs Table over an operator specified time period disclosed in paragraphs 92-93.

In response to applicants' argument that Pruthi does not disclose "a first update period," "a first threshold number 'C1'," and "a first factor value 'C2'," the examiner respectfully points out that Pruthi discloses a time window y in paragraphs 92-93 and 187 that corresponds to "a first update period," a threshold x in paragraph 187 that corresponds to "a first threshold 'C1'," and inherently discloses a historical number of host pairs created by normal operating traffic over the network in paragraph 200 with the difference between the threshold x and the historical number corresponds to "a first factor value 'C2'." The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, through selecting a value for threshold x that is greater than the historical number of host pair connections made by normal operating traffic over the network. This selection allows the for the method of detecting scanning attacks to function properly by alerting the operator when the network is under scanning attacks as opposed to alerting the operator is always under scanning attacks when normal operating traffic is on the network.

The examiner further points out that prior art is presumed to operable and enabled. A reference contains and enabling disclosure if the public was in possession of the claimed invention before the date of invention and such possession is effected if

one of ordinary skill in the art could have combined the publication's description of the invention with his own knowledge to make the claimed invention. See MPEP 2121.01

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Christopher A. Revak/
Primary Examiner, Art Unit 2431